Docket No. 243054US2S

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Toru TERAUCHI

GAU:

SERIAL NO: New Application

EXAMINER:

FILED: Herewith

FOR: METHOD FOR ENCRYPTING CONTENT, AND METHOD AND APPARATUS FOR DECRYPTING ENCRYPTED DATA

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

☐ Full benefit of the filing date of U.S. Application Serial Number , filed , is claimed pursuant to the provisions of **35 U.S.C. §120**.

☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of **35 U.S.C. §119(e)**: **Application No.** **Date Filed**

■ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of **35 U.S.C. §119**, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

COUNTRY	APPLICATION NUMBER	MONTH/DAY/YEAR
Japan	2002-305970	October 21, 2002

Certified copies of the corresponding Convention Application(s)

■ are submitted herewith

☐ will be submitted prior to payment of the Final Fee

☐ were filed in prior application Serial No. filed

☐ were submitted to the International Bureau in PCT Application Number
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and

☐ (B) Application Serial No.(s)

- ☐ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Marvin J. Spivak
Registration No. 24,913

C. Irvin McClelland
Registration Number 21,124

Customer Number
22850
Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 05/03)

035 0341

日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００２年１０月２１日

出願番号
Application Number: 特願２００２－３０５９７０

[ST.10/C]: [ＪＰ２００２－３０５９７０]

出願人
Applicant(s): 株式会社東芝

２００３年　３月１４日

特許庁長官
Commissioner,
Japan Patent Office 太田信一郎

出証番号　出証特２００３－３０１６６１５

【書類名】　特許願

【整理番号】　A000200284

【提出日】　平成14年10月21日

【あて先】　特許庁長官　殿

【国際特許分類】　G09C　1/00

【発明の名称】　コンテンツの暗号化方法及び暗号化されたデータを復号化する復号化方法並びにその装置

【請求項の数】　24

【発明者】

【住所又は居所】　東京都青梅市末広町２丁目９番地　株式会社東芝青梅工場内

【氏名】　寺内　亨

【特許出願人】

【識別番号】　000003078

【氏名又は名称】　株式会社　東芝

【代理人】

【識別番号】　100058479

【弁理士】

【氏名又は名称】　鈴江　武彦

【電話番号】　03-3502-3181

【選任した代理人】

【識別番号】　100084618

【弁理士】

【氏名又は名称】　村松　貞男

【選任した代理人】

【識別番号】　100068814

【弁理士】

【氏名又は名称】　坪井　淳

出証特２００３－３０１６６１５

【選任した代理人】

【識別番号】　100092196

【弁理士】

【氏名又は名称】　橋本　良郎

【選任した代理人】

【識別番号】　100091351

【弁理士】

【氏名又は名称】　河野　哲

【選任した代理人】

【識別番号】　100088683

【弁理士】

【氏名又は名称】　中村　誠

【選任した代理人】

【識別番号】　100070437

【弁理士】

【氏名又は名称】　河井　将次

【手数料の表示】

【予納台帳番号】　011567

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　　コンテンツの暗号化方法及び暗号化されたデータを復号化する復号化方法並びにその装置

【特許請求の範囲】

【請求項１】

コンテンツ毎にユニークに決まるタイトルキーと端末側から取得された項目情報を含みコンテンツの再生対象を限定する再生対象固有情報とが組み合わされた運用規則情報と、

前記タイトルキーと前記再生対象固有情報とから生成される暗号化キー情報を基に暗号化されている暗号化コンテンツ・データとを受け取り、

前記運用規則情報から端末側で取得可能な項目情報を基に暗号化コンテンツ・データの再生可能性を判定し、この判定に従って、前記項目情報及びタイトルキーから復号化キーを生成する復号化キー生成部と、

前記コンテンツ・データを前記復号化キー情報を基に復号化する復号化部と、

を具備する暗号化されたデータを復号化する端末装置。

【請求項２】

前記再生対象固有情報は、再生対象のコンテンツに関する制限項目、前記端末装置を限定する限定項目及びユーザに固有の項目のいずれかの項目を含むことを特徴とする請求項１の端末装置。

【請求項３】

前記暗号化キー情報は、前記再生対象固有情報に依存しない運用規則情報である旨を示すフラグを含むことを特徴とする請求項１の端末装置。

【請求項４】

コンテンツ毎にユニークに決まるタイトルキーと端末側から取得された項目情報を含みコンテンツの再生対象を限定する再生対象固有情報とを基に暗号化したキーワード情報とが組み合わされた運用規則情報と、

前記タイトルキーと前記再生対象固有情報から生成される暗号化キー情報を基に暗号化されている暗号化コンテンツ・データとを受け取り、

前記運用規則情報に含まれる暗号化されたキーワード情報から端末で取得可能

な項目情報を基に暗号化コンテンツ・データの再生可能性を判定し、この判定に従って、前記項目情報及びタイトルキーから復号化キーを生成する復号化キー生成部と、

前記コンテンツ・データを前記復号化キー情報を基に復号化する復号化部と、

を具備する暗号化されたデータを復号化する端末装置。

【請求項５】

前記再生対象固有情報は、再生対象のコンテンツに関する制限項目、前記端末装置を限定する限定項目及びユーザに固有の項目のいずれかの項目を含むことを特徴とする請求項４の端末装置。

【請求項６】

前記暗号化キー情報は、前記再生対象固有情報に依存しない運用規則情報である旨を示すフラグを含むことを特徴とする請求項４の端末装置。

【請求項７】

コンテンツ毎にユニークに決まるタイトルキー及び端末側から項目情報を取得してコンテンツの再生対象を限定する再生対象固有情報を生成する第１の生成部と、

前記タイトルキー及び再生対象固有情報に基づいて暗号化キー情報を生成する第２の生成部と、

コンテンツ・データを暗号化キー情報で暗号化する暗号化部と、

前記タイトルキー及び再生対象固有情報から運用規則情報を生成する運用規則生成部と、

を具備するコンテンツの暗号化装置。

【請求項８】

前記再生対象固有情報は、再生対象のコンテンツに関する制限項目、前記端末装置を限定する限定項目及びユーザに固有の項目のいずれかの項目を含むことを特徴とする請求項７の暗号化装置。

【請求項９】

前記再生対象固有情報に依存しない運用規則情報である旨を示すフラグが運用規則生成部で生成されることを特徴とする請求項７の暗号化装置。

【請求項１０】

コンテンツ毎にユニークに決まるタイトルキー及び端末側から項目情報を取得してコンテンツの再生対象を限定する再生対象固有情報を生成する第１の生成部と、

前記タイトルキー及び再生対象固有情報に基づいて暗号化キー情報を生成し、また、前記再生対象固有情報を基にキーワードを暗号化した暗号化キーワード情報を生成する第２の生成部と、

コンテンツ・データを暗号化キー情報で暗号化する暗号化部と、

前記タイトルキー及び暗号化キーワード情報から運用規則情報を生成する運用規則生成部と、

を具備するコンテンツの暗号化装置。

【請求項１１】

前記再生対象固有情報は、再生対象のコンテンツに関する制限項目、前記端末装置を限定する限定項目及びユーザに固有の項目のいずれかの項目を含むことを特徴とする請求項１０の暗号化装置。

【請求項１２】

前記再生対象固有情報に依存しない運用規則情報である旨を示すフラグが運用規則生成部で生成されることを特徴とする請求項１１の暗号化装置。

【請求項１３】

コンテンツ毎にユニークに決まるタイトルキーと端末側から取得された項目情報を含み、コンテンツの再生対象を限定する再生対象固有情報とが組み合わされた運用規則情報と、

前記タイトルキーと前記再生対象固有情報から生成される暗号化キー情報を基に暗号化されている暗号化コンテンツ・データとを受け取る工程と、

前記運用規則情報から端末側で取得可能な項目情報を基に暗号化コンテンツ・データの再生可能性を判定し、この判定に従って、前記項目情報及びタイトルキーから復号化キーを生成する復号化キー生成工程と、

前記コンテンツ・データを前記復号化キー情報を基に復号化する復号化工程と

を具備する暗号化されたデータを復号化する方法。

【請求項１４】

前記再生対象固有情報は、再生対象のコンテンツに関する制限項目、前記端末装置を限定する限定項目及びユーザに固有の項目のいずれかの項目を含むことを特徴とする請求項１３の方法。

【請求項１５】

前記運用規則情報は、前記再生対象固有情報に依存しない運用規則情報である旨を示すフラグを含むことを特徴とする請求項１３の方法。

【請求項１６】

コンテンツ毎にユニークに決まるタイトルキーと端末側から取得された項目情報を含みコンテンツの再生対象を限定する再生対象固有情報とを基に暗号化したキーワード情報とが組み合わされた運用規則情報と、

前記タイトルキーと、前記再生対象固有情報から生成される暗号化キー情報を基に暗号化されている暗号化コンテンツ・データとを受け取る工程と、

前記運用規則情報に含まれる暗号化されたキーワード情報から端末側で取得可能な項目情報を基に暗号化コンテンツ・データの再生可能性を判定し、この判定に従って、前記項目情報及びタイトルキーから復号化キーを生成する復号化キー生成工程と、

前記コンテンツ・データを前記復号化キー情報を基に復号化する復号化工程と、

を具備する暗号化されたデータを復号化する方法。

【請求項１７】

前記再生対象固有情報は、再生対象のコンテンツに関する制限項目、前記端末装置を限定する限定項目及びユーザに固有の項目のいずれかの項目を含むことを特徴とする請求項１６の方法。

【請求項１８】

前記運用規則情報は、前記再生対象固有情報に依存しない運用規則情報である旨を示すフラグを含むことを特徴とする請求項１６の方法。

【請求項１９】

コンテンツ毎にユニークに決まるタイトルキー及び端末側から項目情報を取得してコンテンツの再生対象を限定する再生対象固有情報を生成する第１の工程と、

前記タイトルキー及び再生対象固有情報に基づいて暗号化キー情報を生成する第２の生成工程と、

コンテンツ・データを暗号化キー情報で暗号化する暗号化工程と、

前記タイトルキー及び再生対象固有情報から運用規則情報を生成する運用規則情報生成工程と、

を具備するコンテンツの暗号化方法。

【請求項２０】

前記再生対象固有情報は、再生対象のコンテンツに関する制限項目、前記端末装置を限定する限定項目及びユーザに固有の項目のいずれかの項目を含むことを特徴とする請求項１９の暗号化方法。

【請求項２１】

前記再生対象固有情報に依存しない運用規則情報である旨を示すフラグが運用規則生成工程で生成されることを特徴とする請求項１９の暗号化方法。

【請求項２２】

コンテンツ毎にユニークに決まるタイトルキー及び端末側から項目情報を取得してコンテンツの再生対象を限定する再生対象固有情報を生成する第１の生成工程と、

前記タイトルキー及び再生対象固有情報に基づいて暗号化キー情報を生成し、また、前記再生対象固有情報を基にキーワードを暗号化した暗号化キーワード情報を生成する第２の生成工程と、

コンテンツ・データを暗号化キー情報で暗号化する暗号化工程と、

前記タイトルキー及び暗号化キーワード情報から運用規則情報を生成する運用規則情報生成工程と、

を具備するコンテンツの暗号化方法。

【請求項２３】

前記再生対象固有情報は、再生対象のコンテンツに関する制限項目、前記端

末装置を限定する限定項目及びユーザに固有の項目のいずれかの項目を含むことを特徴とする請求項２２の暗号化方法。

【請求項２４】

前記再生対象固有情報に依存しない運用規則情報である旨を示すフラグが運用規則生成工程で生成されることを特徴とする請求項２２の暗号化方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は、コンテンツ・データを暗号化する暗号化方法及び暗号化されたデータを復号化する方法に係り、特に、音楽や映像の配信サービスにおける著作権保護方式にて利用される暗号化・復号化方法に関する。

【０００２】

【従来の技術】

近年、インターネット、或いは、携帯電話サービスの普及に伴い、音楽、或いは、映像コンテンツの配信サービスが普及し始めている。このようなサービスにおいては、配信するコンテンツの違法コピーを防ぐために、著作権保護の仕組みが組み込まれている。

【０００３】

著作権保護方式では、一般的に、あるキー情報を元にコンテンツを暗号化した上で配信し、正規ユーザは、正しいキー情報を受け取った上でこのキー情報を元にコンテンツを復号化し、再生している。暗号化されたコンテンツを不正にコピーした場合には、正しいキー情報を受け取れなくすることにより、コンテンツを正しく復号化できなくして、結果として不正に再生することを防止している。

【０００４】

通常のサービスでは、こうしたキー情報の他に、運用規則情報と呼ばれる付加的な情報をやりとりすることで、配信したコンテンツのコピー条件や再生条件などを制限することができる。例えば、再生回数を制限したい場合には、再生可能な回数をあらかじめ設定しておき、運用規則情報として組み込んでいる。コンテンツを配信する際には、暗号化されたコンテンツとペアで、キー情報及び運用規

則情報を配信している。配信先では、受け取ったキー情報を元にコンテンツを復号化し、再生準備をするとともに、同時に、運用規則情報を解析し、再生可能回数を調べている。再生可能回数が１以上であれば、再生処理を実行するとともに、同時に、再生可能回数を１減じた後、その値を運用規則情報に反映している。再生可能回数が０であれば、再生処理を中止している。このように、予め指定された回数だけしか再生できないコンテンツを配信することが可能となる。

【０００５】

こうしたキー情報、或いは、運用規則情報は、コンテンツ配信サービスにおいては、重要な情報であるため、別途セキュリティを考慮した方式で配信される。例えば、インターネットなどの場合、SSL（Secure Sockets Layer）と呼ばれる方式を用いて、運用規則情報が暗号化されて送受信される。

【０００６】

通常、キー情報は、コンテンツ毎にユニークとなるよう、乱数発生器などを用いて生成されたタイトルキーと呼ばれる情報が用いられる。また、タイトルキーと他の情報を組み合わせることで、コンテンツの再生を特定の端末などに限定することができる。例えば、配信元では、再生対象となる端末の製造番号を入手し、タイトルキーと組み合わせてキー情報を生成し、キー情報を用いてコンテンツを暗号化している。配信元は、配信先へタイトルキー及び暗号化コンテンツを配信している。配信先でコンテンツを再生する際には、再生端末に付けられている製造番号と、タイトルキーとが組み合わされてキー情報が生成され、キー情報を用いてコンテンツを復号化した上、コンテンツの再生処理がなされる。このとき、再生端末が配信側で予定している端末でない場合には、予定していない端末に付けられた製造番号及びタイトルキーの組み合わせで生成されるキー情報が不正なものとなるため、コンテンツを正しく復号化することができない。

【０００７】

このように、タイトルキー及び限定対象となる固有情報が組み合わされることで、コンテンツの再生できる対象を限定することが可能となる。限定対象としては、再生する端末を限定する場合、再生する個人を限定する場合、蓄積する媒体を限定する場合、あるいはそれらを組み合わせた場合など、様々な場合が想定さ

れる。

【０００８】

【発明が解決しようとする課題】

しかしながら、上記した従来技術においては、コンテンツの再生対象を限定した場合、コンテンツの再生条件を満たしているかどうかは、コンテンツを復号化するまで判断ができない問題がある。また、コンテンツの種類によっては、例えば、ＰＣＭ（Pulse Code Modulation）生データのようにデータの中身を見ただけでは正しいかどうか判断ができないようなフォーマットの場合、復号化した結果が正しいかどうか判断できない問題がある。

【０００９】

この発明は、上記の問題を解決するためになされたものであり、その目的は、コンテンツの再生対象を限定した場合においても、コンテンツを再生する際に、再生条件を満たしているかどうかを、コンテンツを復号化しなくても確実に判断できる暗号化方法及び暗号化されたコンテンツを復号化する復号化方法を提供するにある。

【００１０】

【課題を解決するための手段】

この発明によれば、

コンテンツ毎にユニークに決まるタイトルキーと端末側から取得された項目情報を含みコンテンツの再生対象を限定する再生対象固有情報とが組み合わされた運用規則情報と、

前記タイトルキーと前記再生対象固有情報とから生成される暗号化キー情報を基に暗号化されている暗号化コンテンツ・データとを受け取り、

前記運用規則情報から端末側で取得可能な項目情報を基に暗号化コンテンツ・データの再生可能性を判定し、この判定に従って、前記項目情報及びタイトルキーから復号化キーを生成する復号化キー生成部と、

前記コンテンツ・データを前記復号化キー情報を基に復号化する復号化部と、

を具備する暗号化されたデータを復号化する端末装置が提供される。

【００１１】

また、この発明によれば、

コンテンツ毎にユニークに決まるタイトルキーと端末側から取得された項目情報を含みコンテンツの再生対象を限定する再生対象固有情報とを基に暗号化したキーワード情報とが組み合わされた運用規則情報と、

前記タイトルキーと前記再生対象固有情報から生成される暗号化キー情報を基に暗号化されている暗号化コンテンツ・データとを受け取り、

前記運用規則情報に含まれる暗号化されたキーワード情報から端末で取得可能な項目情報を基に暗号化コンテンツ・データの再生可能性を判定し、この判定に従って、前記項目情報及びタイトルキーから復号化キーを生成する復号化キー生成部と、

前記コンテンツ・データを前記復号化キー情報を基に復号化する復号化部と、

を具備する暗号化されたデータを復号化する端末装置が提供される。

【００１２】

この発明によれば、また、

コンテンツ毎にユニークに決まるタイトルキー及び端末側から項目情報を取得してコンテンツの再生対象を限定する再生対象固有情報を生成する第１の生成部と、

前記タイトルキー及び再生対象固有情報に基づいて暗号化キー情報を生成する第２の生成部と、

コンテンツ・データを暗号化キー情報で暗号化する暗号化部と、

前記タイトルキー及び再生対象固有情報から運用規則情報を生成する運用規則生成部と、

を具備するコンテンツの暗号化装置が提供される。

【００１３】

更に、この発明によれば、

コンテンツ毎にユニークに決まるタイトルキー及び端末側から項目情報を取得してコンテンツの再生対象を限定する再生対象固有情報を生成する第１の生成部と、

前記タイトルキー及び再生対象固有情報に基づいて暗号化キー情報を生成し、

また、前記再生対象固有情報を基にキーワードを暗号化した暗号化キーワード情報を生成する第２の生成部と、

コンテンツ・データを暗号化キー情報で暗号化する暗号化部と、

前記タイトルキー及び暗号化キーワード情報から運用規則情報を生成する運用規則生成部と、

を具備するコンテンツの暗号化装置が提供される。

【００１４】

また、更にこの発明によれば、

コンテンツ毎にユニークに決まるタイトルキーと端末側から取得された項目情報を含み、コンテンツの再生対象を限定する再生対象固有情報とが組み合わされた運用規則情報と、

前記タイトルキーと前記再生対象固有情報から生成される暗号化キー情報を基に暗号化されている暗号化コンテンツ・データとを受け取る工程と、

前記運用規則情報から端末側で取得可能な項目情報を基に暗号化コンテンツ・データの再生可能性を判定し、この判定に従って、前記項目情報及びタイトルキーから復号化キーを生成する復号化キー生成工程と、

前記コンテンツ・データを前記復号化キー情報を基に復号化する復号化工程と

、

を具備する暗号化されたデータを復号化する方法が提供される。

【００１５】

更にまた、この発明によれば、

コンテンツ毎にユニークに決まるタイトルキーと端末側から取得された項目情報を含みコンテンツの再生対象を限定する再生対象固有情報とを基に暗号化したキーワード情報とが組み合わされた運用規則情報と、

前記タイトルキーと、前記再生対象固有情報から生成される暗号化キー情報を基に暗号化されている暗号化コンテンツ・データとを受け取る工程と、

前記運用規則情報に含まれる暗号化されたキーワード情報から端末側で取得可能な項目情報を基に暗号化コンテンツ・データの再生可能性を判定し、この判定に従って、前記項目情報及びタイトルキーから復号化キーを生成する復号化キー

生成工程と、

前記コンテンツ・データを前記復号化キー情報を基に復号化する復号化工程と、

を具備する暗号化されたデータを復号化する方法が提供される。

【００１６】

また、更に、この発明によれば、

コンテンツ毎にユニークに決まるタイトルキー及び端末側から項目情報を取得してコンテンツの再生対象を限定する再生対象固有情報を生成する第１の工程と、

前記タイトルキー及び再生対象固有情報に基づいて暗号化キー情報を生成する第２の生成工程と、

コンテンツ・データを暗号化キー情報で暗号化する暗号化工程と、

前記タイトルキー及び再生対象固有情報から運用規則情報を生成する運用規則情報生成工程と、

を具備するコンテンツの暗号化方法が提供される。

【００１７】

【発明の実施の形態】

以下、図面を参照しながらこの発明の実施例に係るコンテンツの暗号化方法及び暗号化されたコンテンツを復号化する復号化方法ついて説明する。

【００１８】

図１は、この発明の一実施例に係る暗号化処理の為の回路構成を機能ブロックで示すコンテンツ暗号化処理回路である。図１に示される回路においては、コンテンツ・データが暗号化部１１０に入力されて暗号化されて暗号化コンテンツ・ファイルとして出力される。ここで、コンテンツ・データは、暗号化部１１０において、暗号化キー生成部１１４で生成される暗号化キーに基づいて暗号化される。この暗号化キーは、コンテンツのタイトル毎に定まるタイトルキー及び再生対象固有情報に基づいて暗号化キー生成部１１４で生成される。タイトルキーは、タイトルキー生成部１１６でタイトル毎に生成される。再生対象固有情報は、コンテンツの配布条件に相当する再生対象条件を設定する再生対象条件設定部１

２０からの再生対象条件、コンテンツを再生する機器を限定する端末限定項目情報設定部１２２からの端末限定項目情報及び個人に固有の情報に基づいてコンテンツの再生を限定する個人固有項目情報設定部１２４からの個人固有項目情報が再生対象固有情報生成部１１８に与えられて生成される。再生対象条件設定部１２０、端末限定項目情報設定部１２２及び個人固有項目情報設定部１２４は、再生対象制限項目情報、端末情報及び個人固有項目情報が入出力部（図示せず）を介して供給されるメモリ上の領域が相当し、再生対象固有情報生成部１１８に与えられる情報は、これらの情報に限定されず、他の情報に代えられても、或いは、他の情報が追加されても良い。

【００１９】

タイトルキー生成部１１６で生成されるタイトルキー及び再生対象固有情報生成部１１８で生成される再生対象固有情報は、運用規則情報生成部１１２に与えられて運用規則情報としてファイル化され、この運用規則情報ファイルが出力される。

【００２０】

図２は、図１に示されたコンテンツ暗号化処理回路からの暗号化された暗号化コンテンツ・ファイルを処理する端末の回路構成を機能ブロックで示している。暗号化コンテンツ・ファイル及び運用規則情報ファイルは、ネット網等の通信網を介して送られ、端末の入出力部（図示せず）を介して分離部１４２に与えられる。受信した暗号化コンテンツ・ファイルは、暗号化コンテンツ・データ記憶部１４６に格納され、受信した運用規則情報ファイルは、運用情報記憶部１４４に格納される。これら記憶部は、通常、メモリ上の領域に相当している。図２に示される復号化キー生成部１４８には、端末の固有情報が供給され、また、端末上で入力された個人情報が供給され、復号化キー生成部１４８は、これら端末固有情報及び個人情報並びに運用情報から復号化キーを後に説明するように生成している。復号化部１５０では、暗号化キー生成部１４８で生成された復号化キーを用いて暗号化コンテンツデータを復号化して図示しない変換部で音声信号及び映像信号に変換されて音声・映像コンテンツとして再生される。

【００２１】

次に図１及び図２に示したコンテンツ暗号化処理回路及び端末回路での処理について図３から図５を参照して説明する。

【００２２】

図３は、この発明の一実施例に係る暗号化処理の手順を示すフローチャートである。コンテンツが暗号化される際には、ステップＳ１１に示すように、始めにコンテンツ毎にユニークに決まる固定長のデータがタイトルキーとしてタイトルキー生成部１１６において生成される。例えば、乱数発生器を用いて６４ｂｉｔの乱数データが生成され、タイトルキーに定められる。次に、ステップＳ１２に示すように、コンテンツの再生対象を制限するかどうか、また、制限する場合にはどのような組み合わせで制限するかのような再生対象条件が再生対象条件設定部１２０において設定される。この再生対象条件は、コンテンツ毎にコンテンツの配布元（コンテンツ・プロバイダ）により任意に決められる。次に、ステップＳ１３に示すように設定された再生対象条件が端末に限定されるかどうかが判定され、端末に限定する場合には、ステップＳ１４に示すように対象となる端末の固有情報が端末限定項目情報設定部１２２で入手される。端末の固有情報としては、例えば、端末の製造番号等があり、端末毎にユニークに決まる情報が固有情報として利用される。ステップＳ１５に示すように入手した端末の固有情報は、再生対象固有情報として設定される。

【００２３】

ステップＳ１３において、設定された再生対象条件が端末に限定されない場合には、同様に、ステップＳ１６において、設定された再生対象条件が個人に限定されるかどうかが判定される。個人に限定される場合には、ステップＳ１７に示すように、対象となる個人の固有情報が個人固有項目情報設定部１２４で入手される。この個人情報としては、例えば、クレジットカード番号等があり、個人毎にユニークに決まる情報が固有情報として利用される。入手した個人の固有情報は、ステップＳ１８において、再生対象固有情報として設定される。

【００２４】

ステップＳ１６において、設定された再生対象条件が個人に限定されない場合には、ステップＳ１９に示すように、設定された再生対象条件が端末と個人の組

み合わせに限定されるかどうかが判定される。端末と個人の組み合わせに限定する場合には、ステップＳ２０及びＳ２１に示すように対象となる端末の固有情報が入手されると共に個人の固有情報が入手される。入手した端末の固有情報及び個人の固有情報を基にしてステップＳ２２に示すように再生対象固有情報が再生対象固有情報生成部１１８において生成される。この再生対象固有情報としては、例えば、端末固有情報及び個人固有項目情報をＸＯＲ演算処理した演算結果があり、この演算結果が再生対象固有情報に定められる。

【００２５】

ステップＳ１３、ステップＳ１６及びステップＳ１９のいずれかにおいて、再生対象条件を限定する場合には、ステップＳ２３に示すようにタイトルキー及び再生対象固有情報から暗号化キーが暗号化キー生成部１１４において生成される。この暗号化キーとしては、例えば、タイトルキー及び再生対象固有情報をＸＯＲ演算処理した演算結果があり、この演算結果が暗号化キーに定められる。

【００２６】

ステップＳ１９において、設定された再生対象条件が端末と個人の組み合わせに限定されない場合には、ステップＳ２４に示されるように設定された再生対象条件が限定なしかどうかが判定され、再生対象が限定されない場合には、ステップＳ２５において、タイトルキーがそのまま暗号化キーとして設定される。

【００２７】

ステップＳ２４において、設定された再生対象条件が、上記以外の場合には、ステップＳ２６に示すように判定処理エラーとしてエラー処理がなされ、処理が終了する。

【００２８】

ステップＳ２３において、暗号化キーが設定されると、ステップＳ２７に示すように暗号化部１１０にコンテンツが読み込まれてステップＳ２８に示すように暗号化キーを用いてコンテンツが暗号化処理される。その後、ステップＳ２９に示すように、暗号化されたコンテンツがファイルに書き出される。ステップＳ３０に示すように再生対象固有情報及びタイトルキーが運用規則情報としてファイルに書き出される。

【００２９】

図４には、暗号化処理で生成される運用規則情報のデータ構造が示されている。運用規則情報は、再生対象条件を限定するかどうかを示すフラグ２０１と、再生対象固有情報２０２及びタイトルキー２０３から構成される。再生対象を限定する場合には、再生対象限定フラグに１が設定され、このフラグ「１」によって、再生対象固有情報が有効であることが示される。逆に、再生対象を限定しない場合には、再生対象限定フラグに０が設定され、このフラグ「０」によって、再生対象固有情報が不定となる。暗号化処理で生成された暗号化データと運用規則情報は、サービスに応じてあらかじめ決められた方法で、再生端末へ配信される。

【００３０】

再生端末では、図５に示すような手順に従い暗号化されたコンテンツが復号化処理される。

【００３１】

再生端末では、暗号化コンテンツ・ファイルと運用規則情報ファイルがファイル受信部１４２に入力され、夫々運用規則情報記憶部１４４及び暗号化コンテンツ・データ記憶部１４６に記憶される。復号化キー生成部１４８では、始めにステップＳ３１に示されるように配信された運用規則情報が読み込まれる。次に、ステップＳ３２において、読み込んだ運用規則情報から再生対象限定フラグが抽出され、再生対象限定フラグが１に設定されているかが判断される。フラグに１が設定されている場合には、再生対象が限定されていると判断される。従って、ステップＳ３３に示すように端末固有情報が再生端末から復号化キー生成部１４８に入力される。また、ステップＳ３４に示すように個人固有項目情報が復号化キー生成部１４８に入力される。

【００３２】

次に、読み込んだ運用規則情報から再生対象固有情報が抽出され、ステップＳ３５に示すように再生対象固有情報が端末固有情報と一致するかが判定される。両者が一致しない場合には、ステップＳ３６に示すように同様にして再生対象固有情報が個人固有項目情報と一致するかが判定される。再生対象固有情報が個人

固有項目情報に一致しない場合には、ステップＳ３７において、端末固有情報及び個人固有項目情報から固有情報が復号化キー生成部１４８で生成される。例えば、既に述べたように端末固有情報及び個人固有項目情報がＸＯＲ演算処理され、その演算結果が固有情報として求められる。次に、ステップＳ３８において、再生対象固有情報と生成した固有情報が一致するかが判定される。ステップＳ３５、Ｓ３６、Ｓ３７のいずれかにおいて、運用規則情報内の再生対象固有情報と、上記いずれかの条件が一致される場合には、再生対象であると判断され、ステップＳ３９において、運用規則情報内のタイトルキー及び再生対象固有情報から復号化キーが復号化キー生成部１４８で生成される。例えば、タイトルキー及び再生対象固有情報がＸＯＲ演算処理され、その演算結果が復号化キーとされる。ステップＳ３８に示すように、いずれの条件にも一致されない場合には、ステップＳ４０において、再生対象ではないと判断され、復号処理が中断される。運用規則情報の再生対象制限フラグが１でなかった場合には、ステップＳ４１において、運用規則情報のタイトルキーがそのまま復号化キーとして復号化キー生成部１４８において設定される。復号化キーが設定されると、次に、ステップＳ４２に示すように暗号化されたコンテンツが読み込まれ、ステップＳ４３に示すように復号化キーを用いてコンテンツが復号化部１５０において復号化される。その後、ステップＳ４４において復号化されたコンテンツが書き出され、処理が終了される。

【００３３】

上述した実施例では、再生対象を限定する条件を、限定なし、端末に限定、個人に限定、端末と個人に限定、のいずれかの場合を前提に説明したが、限定条件はこれに限るものではなく、他の限定条件に換えられても、或いは、他の限定条件が付されても良いことは明らかである。

【００３４】

上述した実施例に係るコンテンツの暗号化方法及び暗号化されたコンテンツを復号化する復号化方法によれば、コンテンツが暗号化される際に、再生対象を限定するための固有情報は、再生対象固有情報として運用規則情報に組み込まれ、暗号化コンテンツと共に配信される。また、コンテンツが復号化される際には、

運用規則情報内の再生対象固有情報と、再生元の各種固有情報と比較することによって、再生条件を満たしているかどうかを確実に判断することが可能となり、コンテンツを復号化処理しなくても再生条件を判断することができる。従って、処理の効率化を図ることができる暗号化コンテンツを配信することができ、また、暗号化されたコンテンツの処理の効率化を図ることができる。

【００３５】

次に、この発明の他の実施例に係るコンテンツの暗号化方法及び暗号化されたコンテンツを復号化する復号化方法ついて図６から図９を参照して説明する。

【００３６】

図６は、この発明の他の実施例に係る暗号化処理の為の回路構成を機能ブロックで示すコンテンツ暗号化処理回路である。図６に示される機能ブロック回路は、実質的に図１に示す機能ブロック回路に同一であるので、図１と同一箇所には、同一符号を付してその説明を省略する。

【００３７】

図６に示されるコンテンツ暗号化処理回路では、運用規則情報生成部１１２に代えて暗号化されたキーワードを運用規則情報として生成する運用規則情報生成部１６０が設けられている。即ち、再生対象固有情報生成部１１８からの再生対象固有情報及びタイトルキー生成部１１６からのタイトルキーで暗号化キー生成部１１４で暗号化キーが生成され、また、再生対象固有情報を用いてキーワードが暗号化され、この暗号化キーワードがタイトルキーとともに運用規則情報生成部１６０で運用規則情報ファイルとして書き出される。

【００３８】

暗号化処理手順を示すフローチャートを示す図７を参照して図６に示したコンテンツ暗号化処理回路での暗号化処理について説明する。

【００３９】

図７に示されるコンテンツを暗号化する手順は、図１～図３を参照して説明した第１実施例の暗号化処理とほぼ同一の手順で実行される。従って、図４において、図１に付した符号と同一の符号を付した処理は、同一の処理が実行されるものとしてその説明を省略する。

【００４０】

この他の実施例に係るコンテンツの暗号化方法においては、ステップＳ１１からＳ２３が実行されて再生対象条件が限定されてタイトルキー及び再生対象固有情報から暗号化キーが生成された後に、第１の実施例と異なり、ステップＳ５１において、暗号化キー生成部１１４において、再生対象固有情報をキーとしてあらかじめ決められているキーワードが暗号化される。例えば、０ｘ１２３４５６７８というキーワード値が再生対象固有情報をキーとして暗号化される。そして、以下同様にステップＳ２７～Ｓ３０の処理が実行され、暗号化されたキーワードが運用規則情報生成部１６０に書き出され、この運用規則情報生成部１６０において、暗号化されたキーワード情報及びタイトルキーが運用規則情報ファイルとして書き出される。

【００４１】

図８には、暗号化処理で生成される運用規則情報のデータ構造が示されている。運用規則情報は、再生対象条件を限定するかどうかを示すフラグ５０１と、暗号化されたキーワード情報５０２、タイトルキー５０３から構成される。再生対象を限定する場合には、再生対象限定フラグに１が設定され、このフラグ「１」によって、暗号化されたキーワード情報が有効であることが示される。逆に、再生対象を限定しない場合には、再生対象限定フラグに０が設定され、このフラグ「０」によって、暗号化されたキーワード情報が不定となる。暗号化処理で生成された暗号化データ及び運用規則情報は、サービスに応じてあらかじめ決められた方法で、再生端末へ配信される。

【００４２】

図２に示す再生端末では、図９に示すような手順に従い暗号化コンテンツが復号化処理される。図９に示される処理においては、図５に示したと同様の処理を含むことからおいて、図５に付した符号と同一の符号を付した処理は、同一の処理が実行されるものとしてその説明を簡略にして説明する。

【００４３】

始めに、ステップＳ３１において、配信された運用規則情報が読み込まれる。次に、運用情報記憶部１４４に読み込こまれた運用規則情報から再生対象限定フ

ラグが復号化キー生成部１４８で抽出され、ステップＳ３２において、再生対象限定フラグが１に設定されているかが判断される。フラグに１が設定されている場合、再生対象が限定されているものと判断され、ステップＳ３３において、復号化キー生成部１４８に端末固有情報が再生端末から入力され、ステップＳ３４において、個人固有項目情報が同様に入力される。

【００４４】

ここで、図６に示す処理においては、ステップＳ６５に示されるように、端末固有情報が再生対象固有情報として復号化キー生成部１４８においてにおいて設定される。次に、ステップＳ６６において、再生対象固有情報をキーにして、運用規則情報内の暗号化キーワード情報が復号化キー生成部１４８において復号化処理され、ステップＳ６７において、復号化されたキーワード情報があらかじめ決められたキーワード情報、例えば０ｘ１２３４５６７８と一致するかが判定される。両者が一致しない場合には、ステップＳ６８において、個人固有項目情報が再生対象固有情報として設定される。次に、ステップＳ６９において、再生対象固有情報をキーにして、復号化キー生成部１４８において、運用規則情報内の暗号化キーワード情報が復号化処理され、ステップＳ７０において、復号化されたキーワード情報があらかじめ決められたキーワード情報と一致するかが判定される。両者が一致しない場合、ステップＳ７１において、端末固有情報と個人固有項目情報から再生対象固有情報が復号化キー生成部１４８において生成される。例えば、端末固有情報及び個人固有項目情報がＸＯＲ演算処理されて求められた演算結果が再生対象固有情報に定められる。ステップＳ７２において、再生対象固有情報をキーにして、運用規則情報内の暗号化キーワード情報が復号化キー生成部１４８において復号化処理され、ステップＳ７３において、復号化されたキーワード情報があらかじめ決められたキーワード情報と一致するかが判定される。

【００４５】

上記ステップＳ６７、Ｓ７０、Ｓ７３において、いずれかの条件にて、暗号化キーワードからキーワードが復号されている場合には、再生対象であると判断され、ステップＳ３９において、運用規則情報内のタイトルキーと再生対象固有情

報から復号化キーが生成される。例えば、タイトルキー及び再生対象固有情報のＸＯＲ演算処理した演算結果が復号化キーとされる。ステップＳ６７、Ｓ７０、Ｓ７３において、いずれの条件にも一致しなかった場合には、復号化キー生成部１４８において再生対象ではないと判断され、ステップＳ４０において、復号処理が中断される。ステップＳ３２において、運用規則情報の再生対象制限フラグが１でなかった場合には、ステップＳ４１において、運用規則情報のタイトルキーがそのまま復号化キーとして設定される。ステップＳ４１或いはＳ３９において、復号化キーが設定されると、ステップＳ４２において、暗号化されたコンテンツが復号化部１５０に読み込まれ、ステップＳ４３において、復号化キーを用いてコンテンツが復号化される。その後、ステップＳ４４において、復号化されたコンテンツが書き出されて処理が終了される。

【００４６】

この他の実施例では、再生対象を限定する条件を、限定なし、端末に限定、個人に限定、端末と個人に限定、のいずれかの場合を前提に説明したが、限定条件はこれに限るものではなく、他の限定条件に換えられても、或いは、他の限定条件が付されても良いことは明らかである。

【００４７】

以上、図６から図９に示された他の実施例によれば、コンテンツが暗号化される際に、再生対象を限定するための固有情報をキーにキーワードが暗号化され運用規則情報に組み込まれ、暗号化コンテンツと共に配信される。また、コンテンツが復号化される際には、再生元の各種固有情報をキーに運用規則情報内の暗号化キーワードを正しく復号化できるかどうかを判断することで、再生条件を満たしているかどうかを確実に判定することができる。従って、処理の効率化を図ることができる暗号化コンテンツを配信することができ、また、暗号化されたコンテンツの処理の効率化を図ることができる。

【００４８】

【発明の効果】

以上のように、コンテンツの再生対象を限定した場合においても、コンテンツを再生する際に、再生条件を満たしているかどうかを、コンテンツを復号化し

なくても確実に判断できる暗号化方法及び暗号化されたコンテンツを復号化する復号化方法が提供される。

【図面の簡単な説明】

【図１】

この発明の一実施例に係るコンテンツの暗号化方法を実現するための機能ブロックを示す説明図である。

【図２】

この発明の一実施例に係る暗号化されたコンテンツを復号化する復号化方法を実現するための機能ブロックを示す説明図である。

【図３】

この発明の一実施例に係るコンテンツの暗号化方法を示すフローチャートである。

【図４】

図３に示された方法によって作成される運用規則情報ファイルのフォーマットを示す平面図である。

【図５】

この発明の他の実施例に係る暗号化されたコンテンツの復号化方法を示すフローチャートである。

【図６】

この発明の他の実施例に係るコンテンツの暗号化方法を実現するための機能ブロックを示す説明図である。

【図７】

この発明の他の実施例に係るコンテンツの暗号化方法を示すフローチャートである。

【図８】

図７に示された方法によって作成される運用規則情報ファイルのフォーマットを示す平面図である。

【図９】

この発明の他の実施例に係る暗号化されたコンテンツの復号化方法を示すフ

ローチャートである。

【符号の説明】

１１０．．．暗号化部

１１２、１６０．．．運用規則情報生成部

１１４．．．暗号化キー生成部

１１６．．．タイトルキー生成部

１１８．．．再生対象固有情報生成部

１２０．．．再生対象条件設定部

１２４．．．個人固有項目情報設定部

１４２．．．ファイル受信部

１４４．．．運用情報記憶部

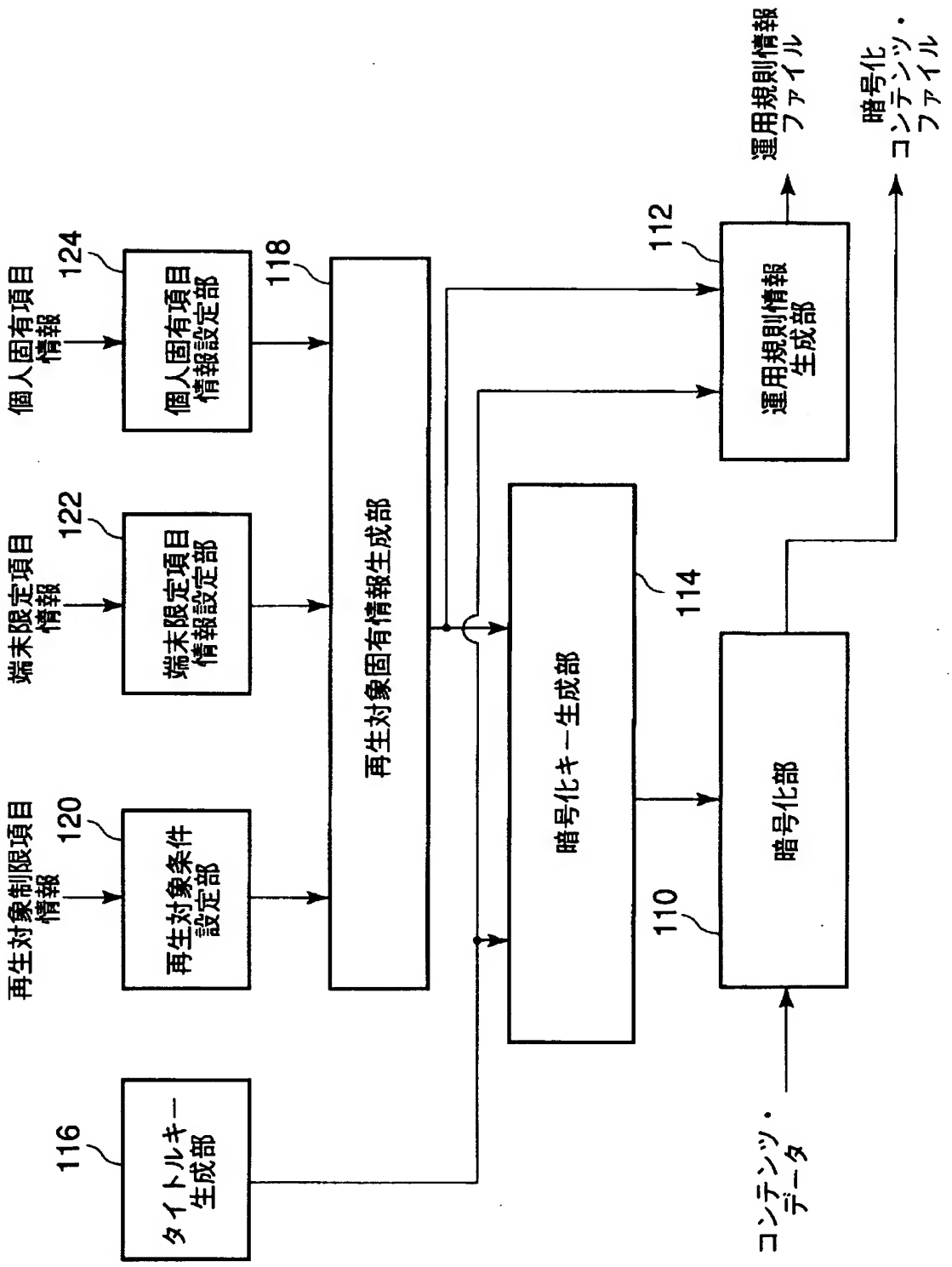
１４６．．．暗号化コンテンツ・データ記憶部

１４８．．．復号化キー生成部

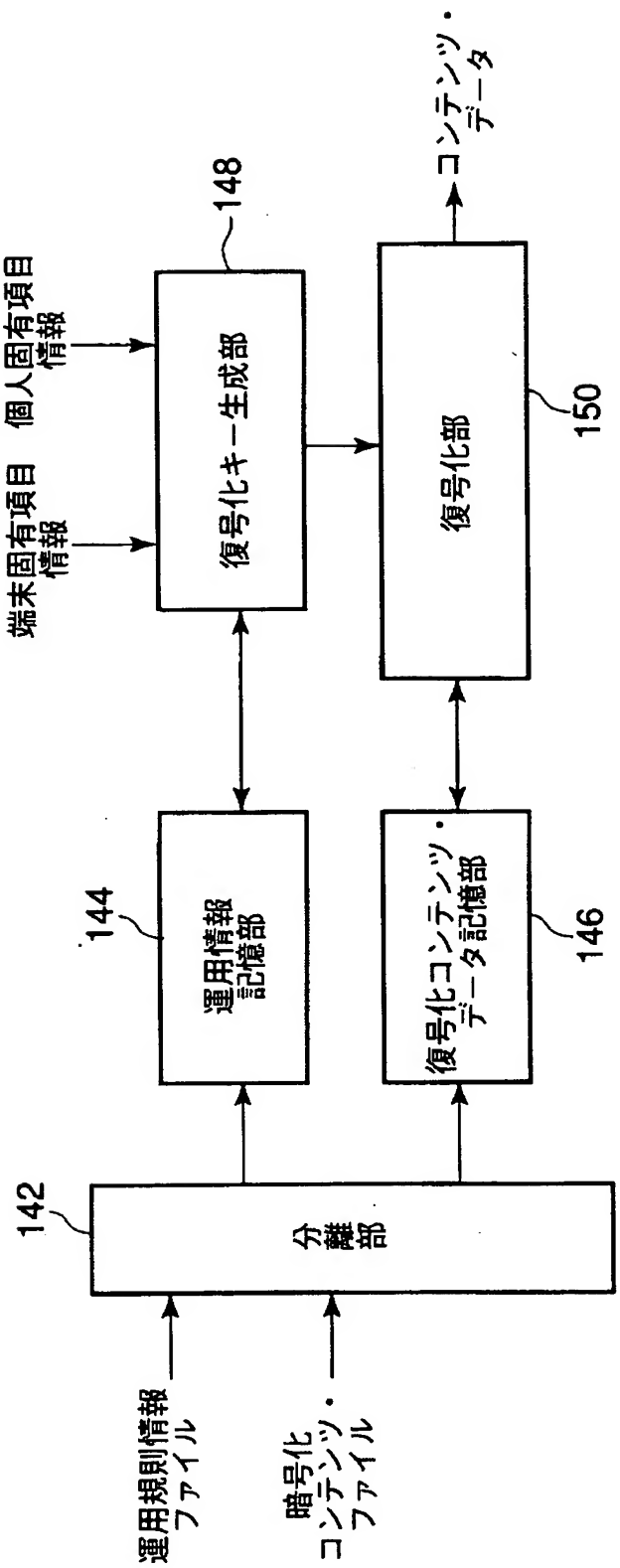
１５０．．．復号化部

【書類名】　　図面

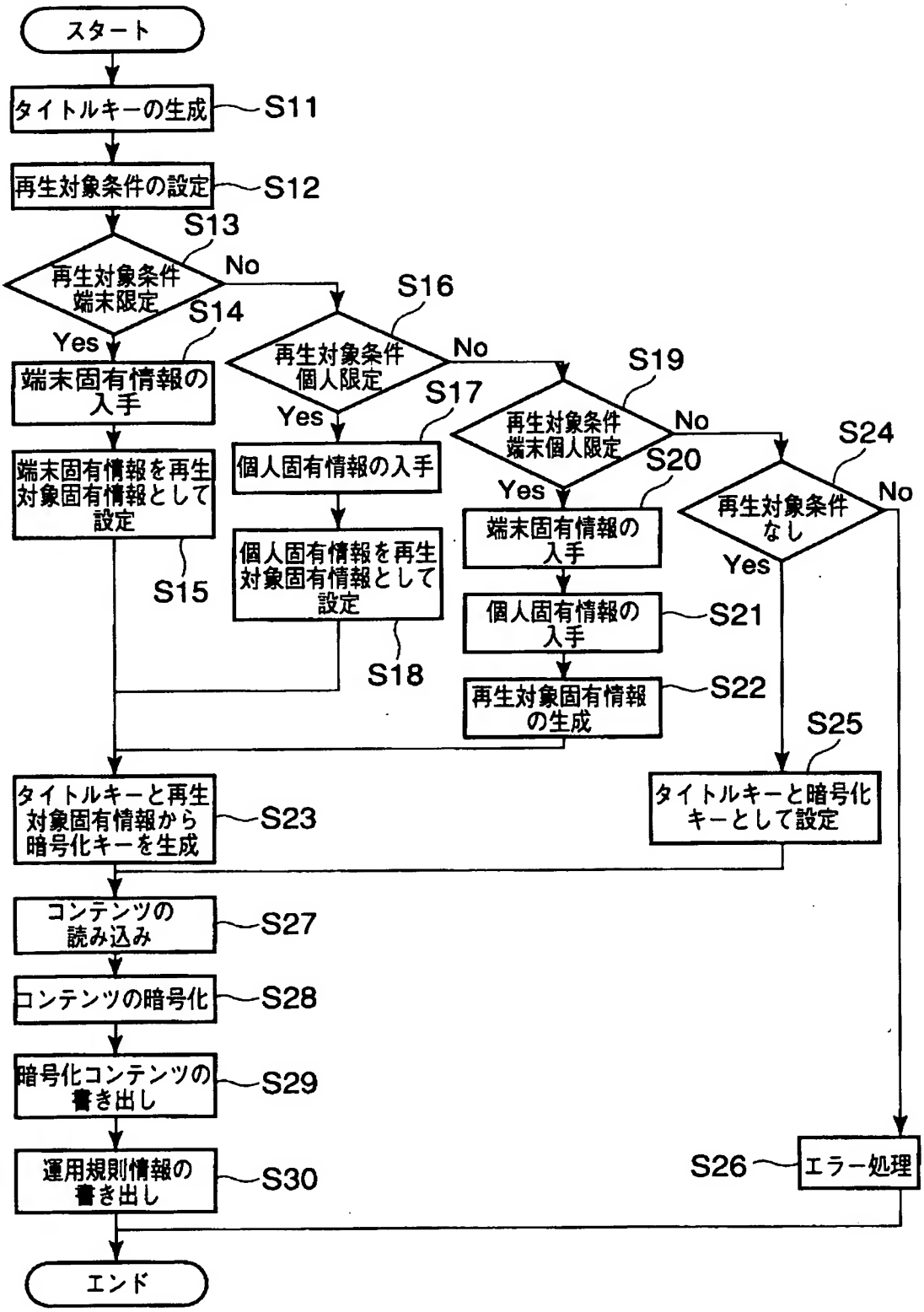
【図１】


個人固有項目情報
124
個人固有項目情報設定部
118
端末限定項目情報
122
端末限定項目情報設定部
再生対象制限項目情報
120
再生対象条件設定部
再生対象固有情報生成部
タイトルキー生成部
116
暗号化キー生成部
114
暗号化部
110
運用規則情報生成部
112
運用規則情報ファイル
暗号化コンテンツ・ファイル
コンテンツ・データ

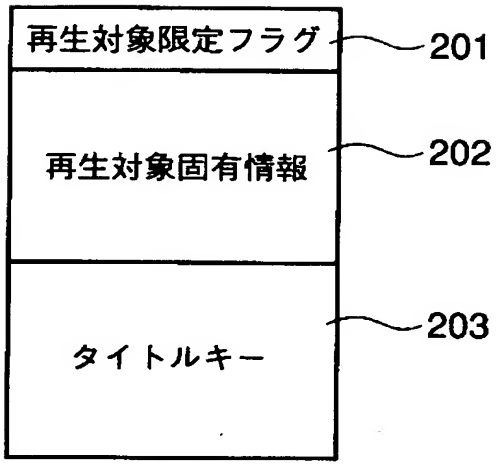
【図２】


コンテンツ・データ
148
個人固有項目情報
端末固有項目情報
復号化キー生成部
復号化部
150
144
運用情報記憶部
復号化コンテンツ・データ記憶部
146
142
分離部
運用規則情報ファイル
暗号化コンテンツ・ファイル

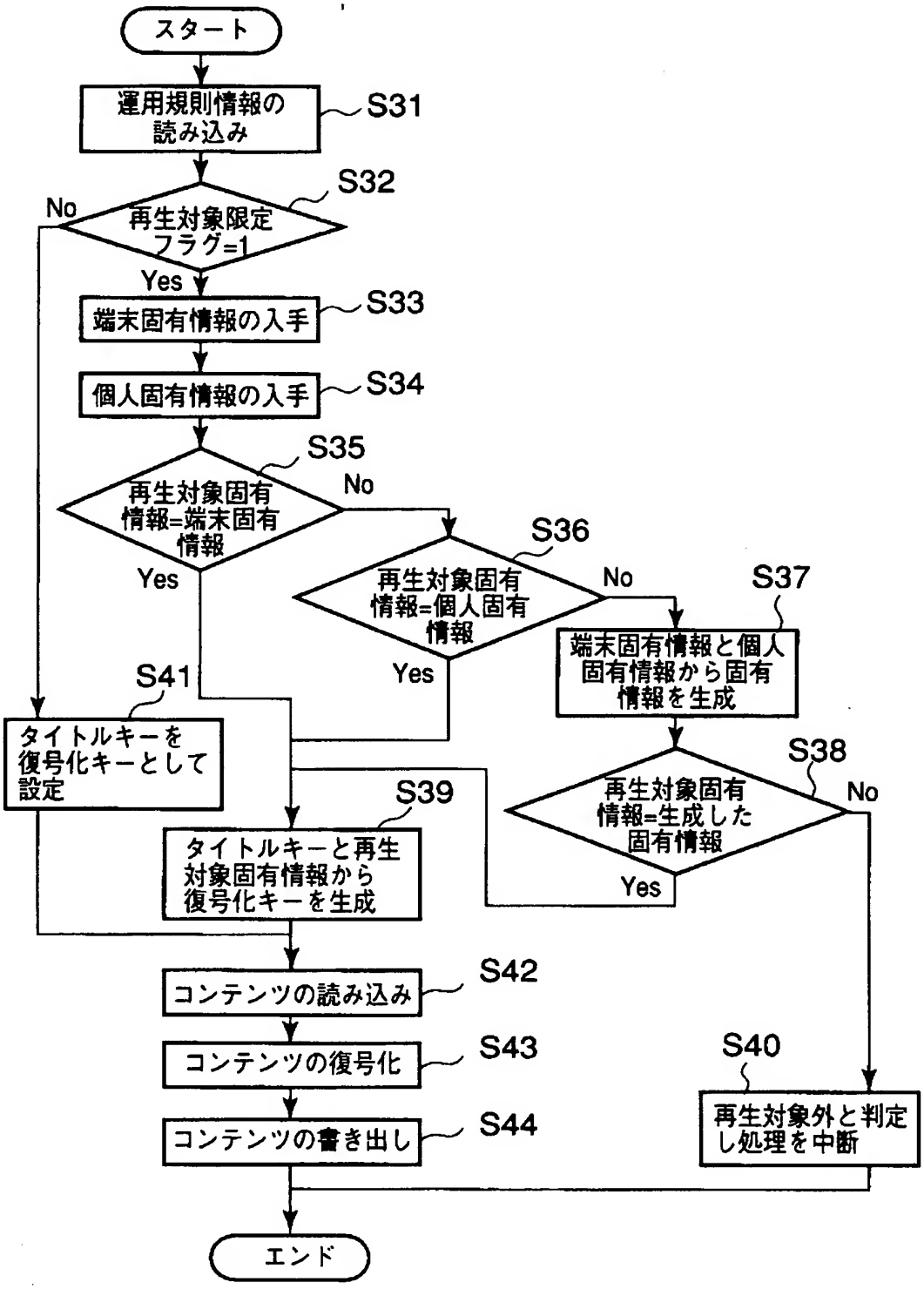
【図３】


スタート
タイトルキーの生成
S11
再生対象条件の設定
S12
S13
再生対象条件
端末限定
No
Yes
S14
端末固有情報の
入手
端末固有情報を再生
対象固有情報として
設定
S15
S16
再生対象条件
個人限定
No
Yes
S17
個人固有情報の入手
個人固有情報を再生
対象固有情報として
設定
S18
S19
再生対象条件
端末個人限定
No
Yes
S20
端末固有情報の
入手
個人固有情報の
入手
S21
再生対象固有情報
の生成
S22
S24
再生対象条件
なし
No
Yes
S25
タイトルキーと暗号化
キーとして設定
タイトルキーと再生
対象固有情報から
暗号化キーを生成
S23
コンテンツの
読み込み
S27
コンテンツの暗号化
S28
暗号化コンテンツの
書き出し
S29
運用規則情報の
書き出し
S30
S26
エラー処理
エンド

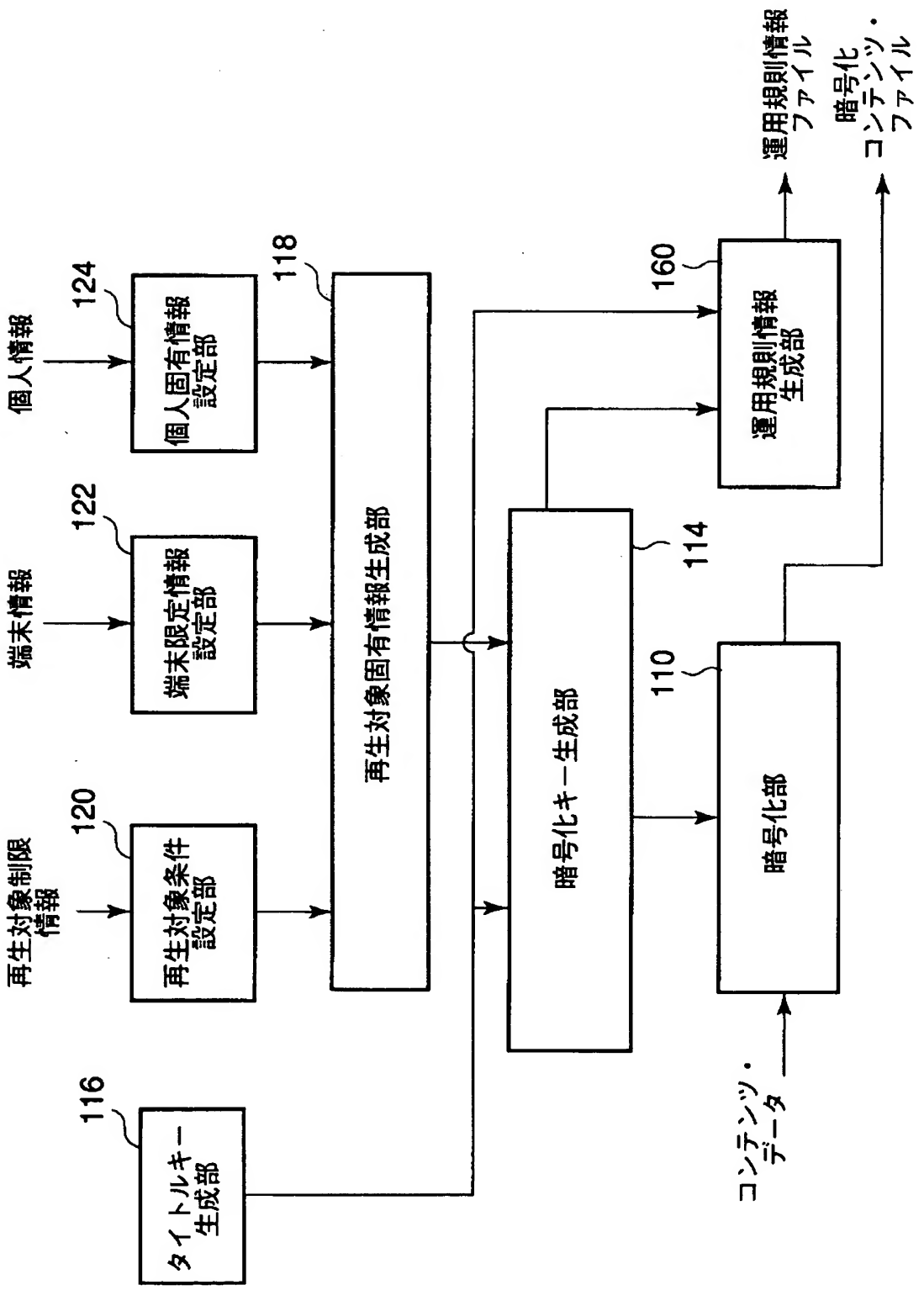
【図４】



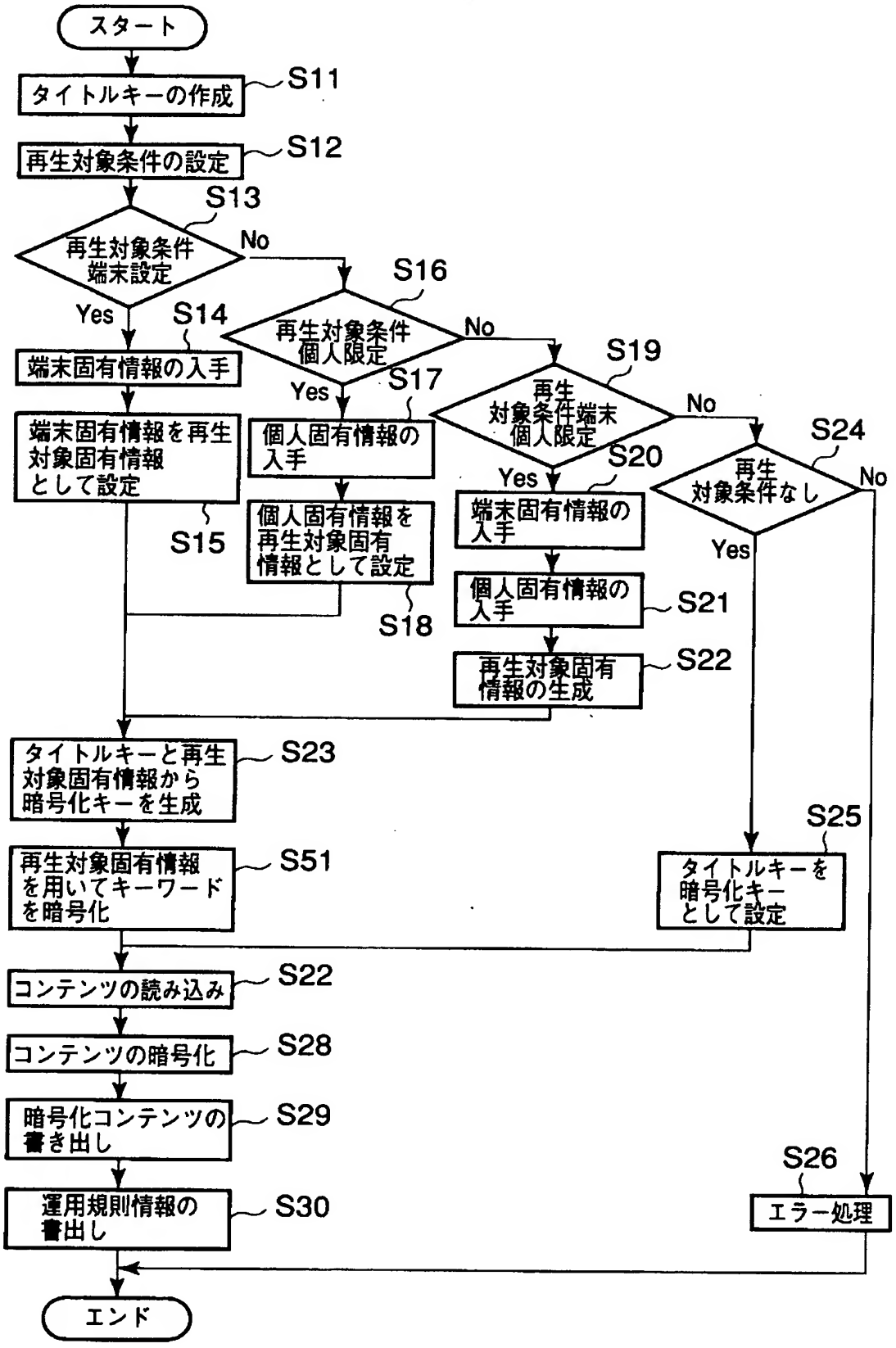
【図５】


スタート
運用規則情報の読み込み
S31
S32
再生対象限定フラグ=1
No
Yes
端末固有情報の入手
S33
個人固有情報の入手
S34
S35
再生対象固有情報=端末固有情報
No
Yes
S36
再生対象固有情報=個人固有情報
No
Yes
S37
端末固有情報と個人固有情報から固有情報を生成
S38
再生対象固有情報=生成した固有情報
No
Yes
S41
タイトルキーを復号化キーとして設定
S39
タイトルキーと再生対象固有情報から復号化キーを生成
S42
コンテンツの読み込み
S43
コンテンツの復号化
S44
コンテンツの書き出し
S40
再生対象外と判定し処理を中断
エンド

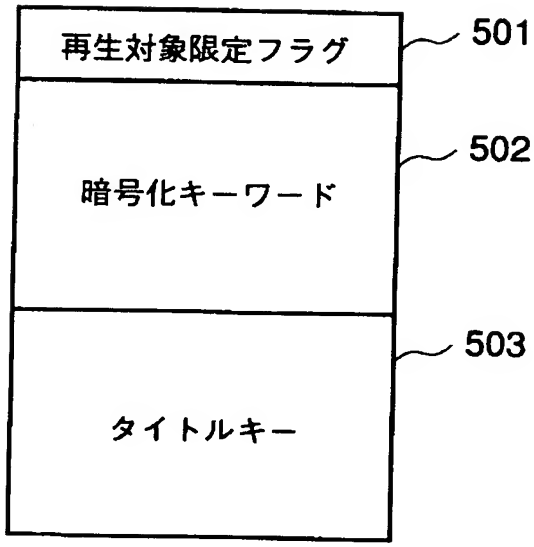
【図６】


個人情報
124
個人固有情報設定部
118
端末情報
122
端末限定情報設定部
再生対象制限情報
120
再生対象条件設定部
再生対象固有情報生成部
116
タイトルキー生成部
暗号化キー生成部
114
160
運用規則情報生成部
110
暗号化部
運用規則情報ファイル
暗号化コンテンツ・ファイル
コンテンツ・データ

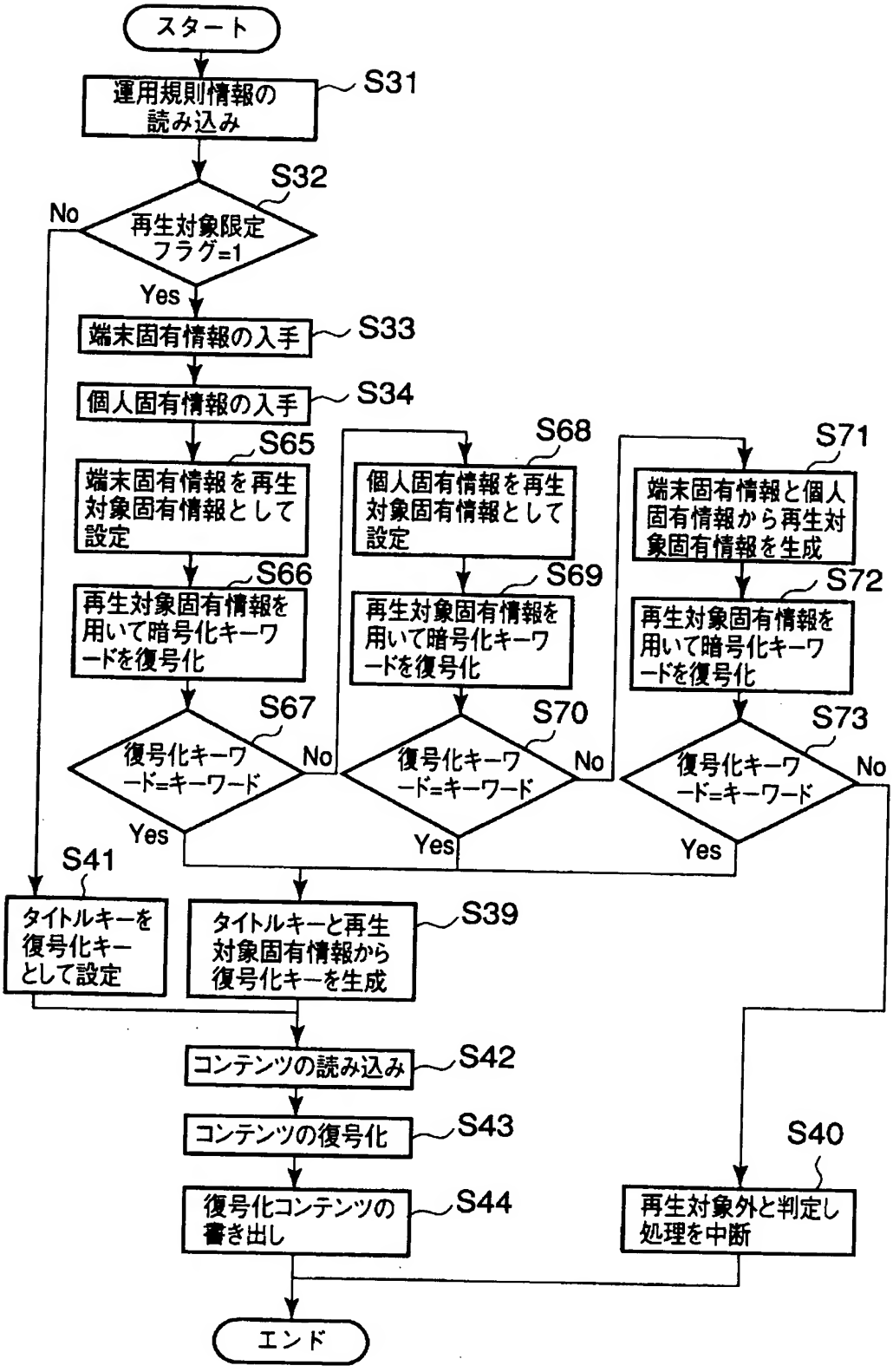
【図７】


スタート
タイトルキーの作成
S11
再生対象条件の設定
S12
S13
再生対象条件端末設定
No
Yes
S14
端末固有情報の入手
端末固有情報を再生対象固有情報として設定
S15
S16
再生対象条件個人限定
No
Yes
S17
個人固有情報の入手
個人固有情報を再生対象固有情報として設定
S18
S19
再生対象条件端末個人限定
No
Yes
S20
端末固有情報の入手
個人固有情報の入手
S21
再生対象固有情報の生成
S22
S24
再生対象条件なし
No
Yes
タイトルキーと再生対象固有情報から暗号化キーを生成
S23
再生対象固有情報を用いてキーワードを暗号化
S51
S25
タイトルキーを暗号化キーとして設定
コンテンツの読み込み
S22
コンテンツの暗号化
S28
暗号化コンテンツの書き出し
S29
運用規則情報の書出し
S30
S26
エラー処理
エンド

【図８】



【図９】


スタート
運用規則情報の読み込み
S31
S32
再生対象限定フラグ=1
No
Yes
端末固有情報の入手
S33
個人固有情報の入手
S34
S65
端末固有情報を再生対象固有情報として設定
S66
再生対象固有情報を用いて暗号化キーワードを復号化
S67
復号化キーワード=キーワード
No
Yes
S68
個人固有情報を再生対象固有情報として設定
S69
再生対象固有情報を用いて暗号化キーワードを復号化
S70
復号化キーワード=キーワード
No
Yes
S71
端末固有情報と個人固有情報から再生対象固有情報を生成
S72
再生対象固有情報を用いて暗号化キーワードを復号化
S73
復号化キーワード=キーワード
No
Yes
S41
タイトルキーを復号化キーとして設定
S39
タイトルキーと再生対象固有情報から復号化キーを生成
コンテンツの読み込み
S42
コンテンツの復号化
S43
復号化コンテンツの書き出し
S44
S40
再生対象外と判定し処理を中断
エンド

【書類名】　　要約書

【要約】

【課題】　コンテンツの再生に際して再生条件を満たしているかどうかを、コンテンツを復号化なしに判断できる復号化方法を提供するにある。

【解決手段】　暗号化データを復号化する方法においては、コンテンツ毎にユニークに決まるタイトルキーと端末を限定する項目情報を含みコンテンツの再生対象を限定する固有情報とが組み合わされた運用規則情報及び前記タイトルキーと前記固有情報から生成される暗号化キー情報とを基に暗号化されている暗号化コンテンツ・データを受け取り、端末側装置から項目情報が取得され、この項目情報と前記運用規則情報とから暗号化コンテンツ・データの再生可能性が判定される。この判定に従って、前記項目情報及びタイトルキーから復号化キーが生成され、コンテンツ・データは、この復号化キー情報を基に復号化される。

【選択図】　　図２

出証特２００３－３０１６６１５

出　願　人　履　歴　情　報

識別番号　　〔０００００３０７８〕

１．変更年月日　　２００１年　７月　２日
［変更理由］　住所変更
住　所　　東京都港区芝浦一丁目１番１号
氏　名　　株式会社東芝

出証特２００３－３０１６６１５